토르 네트워크 상에서의 악성 릴레이 탐지를 위한 행위 특성 분석

이수빈[1], 김다형[1], 유정화[1], 최이슬[2], 김성민[3]
성신여자대학교 융합보안공학과 (학부생)[1], (대학원생)[2], (교수)[3]

Behavioral Characteristic Analysis for Detecting Malicious Relays in the Tor Network

Su-bin Lee[1], Da-hyung Kim[1], Jeong-hwa Ryu[1], Yi-seul Choi[2], Seong-min Kim[3]
[1,2,3]Dept. of Convergence Security Engineering, Sungshin Women's University

요 약

오늘날의 대표적인 익명 네트워크인 토르(Tor)는 자원봉사자의 릴레이에 기반해 운영되며, 이로 인해 악의적 릴레이를 통한 사용자 대상의 능동적(active) 공격 사례가 다수 존재한다. 본 논문은 이러한 공격의 특성을 분석하고, 악성 행위에 따른 릴레이의 특징을 시나리오 기반으로 구분하여 살펴본다. 특히, C&C 서버와의 통신 여부, 대역폭 허위 보고와 같은 행위를 중심으로 분석을 진행하였으며, 연구 결과는 향후 악성 릴레이 탐지에 활용될 수 있을 것으로 기대한다.

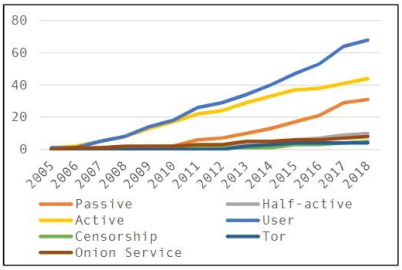
1. 서론

현대 인터넷에서 익명성을 강화하기 위한 가장 대표적인 기술로 자리 잡은 토르는 2억 회 이상 다운로드 될 만큼 활성화되어 있다. 그러나, 대표적인 익명 네트워크로 자리 잡으면서 토르를 대상으로 하는 공격 역시 폭발적으로 증가하였다. 특히, 자원봉사자가 운영하는 릴레이(Relay)를 기반으로 동작[1]하는 토르의 특성상 누구나 릴레이를 등록하거나 수정할 수 있어 악의적인 릴레이를 등록하여 공격에 활용하는 경우가 많다. 따라서, 공격에 활용되는 릴레이를 탐지하여 차단할 필요가 있으며, 이를 위해서는 일반적으로 운영되는 릴레이와의 차이점을 식별해야 한다.

이에 본 논문에서는 악성 행위에 따른 릴레이의 특징을 분석하고자 한다. 분석 결과, 호스트 내 식별 가능한 악성 릴레이 행위 패턴은 공격자가 운용하는 C&C 서버와의 통신과 토르 사용자들로부터의 선택 확률을 높이기 위한 대역폭(Bandwidth) 허위 보고로 크게 나타낼 수 있다. 본 연구에서 제시하는 분석 결과는 추후 토르 네트워크 내 악성 릴레이 탐지를 위한 특징 추출을 위해 활용될 수 있을 것이다.

2. 배경 및 관련 연구

미국 해군 연구소에서 개발한 토르는 어니언 라우팅(Onion Routing)을 기반으로 하여 인터넷 사용자의 신원이 드러나지 않도록 함으로써 익명성을 보장하는 네트워크이다. 입구 릴레이(Entry Relay), 중간 릴레이(Middle Relay), 출구 릴레이(Exit Relay)로 구성되며, 패킷은 각 릴레이를 거칠 때마다 암호화된다. 이때, 각 노드는 직전 노드의 패킷만 복호화하기 때문에 사용자의 IP는 노출되지 않아 익명성이 유지된다[2].



(그림 1) 토르 공격 통계

토르 공격은 대상 구성요소의 수정/변경 여부에 따라 크게 능동적 공격과 수동적(passive) 공격으로 분류할 수 있다. 보고된 결과에 따르면, 이 중 사용자를 대상으로 하는 능동적 공격의 비중이 그림1과 같이 가장 높다[3]. 실제로, 900개가 넘는 악성 릴레이를 등록하여 공격에 활용한 사례가 있다[4]. 따라서, 본 논문에서는 공격에 사용되는 릴레이의 특징

을 분석하여 능동적 탐지에 활용할 수 있도록 한다.

3. 악성 릴레이 특징 분석

본 논문에서는 특정 릴레이를 등록하여 운영하는 호스트 PC에서 악성 릴레이 여부를 판단하는 시나리오를 가정하여, 호스트 내에서 식별 가능한 악성 행위에 따른 특징을 분석한다. 표 1은 악성 행위별 특징 및 호스트 내 의심 지표를 요약한 결과이다.

<표 1> 악성 행위별 특징

유형	특징	의심 지표
C&C 서버와 통신	시스템 로그 및 트래픽에서 정상 릴레이와의 차이 발생	• 자체 서명된 인증서 또는 신뢰할 수 없는 CA에서 발급된 인증서 사용 • 비표준 포트 사용 • 짧은 연결 시간(1분 미만) 다수 발생
대역폭 허위 보고	높은 대역폭 보고로 입/출구 릴레이 선정 확률 증가	• 보고된 대역폭 대비 낮게 기록된 CPU/메모리 사용량 • 다수의 torrc파일 존재

3.1 C&C(Command & Control) 서버와 통신

C&C 서버와 통신하는 릴레이의 경우 시스템 로그와 트래픽에서 정상 릴레이와의 차이를 보인다. 구체적으로, ssl.log에는 TLS/SSL 핸드셰이크 과정에서 사용된 인증서 정보가 기록되며, 이 중 공인 CA가 아닌 자체 서명된 인증서 또는 신뢰할 수 없는 CA에서 발급된 인증서가 사용된 경우 악성 릴레이임을 의심할 수 있다. 또한, 표준 토르 포트인 9001, 9010, 443, 9050, 9150, 443, 80, 8080 외 포트를 사용할 수 있다.

추가로, 정상 릴레이의 경우, 평균 5분 이상의 연결 지속 시간을 갖지만, C&C 서버와 통신하는 경우 빠른 명령 실행, 상태 보고, 또는 데이터 전송과 같은 목적을 위해 1분 미만의 짧은 연결이 다수 발생할 수 있다. 이는 악성 릴레이가 서버와의 지속적인 연결을 최소화하고 탐지를 회피하기 위해 짧은 시간 내에 명령을 처리하고 연결을 종료하는 방식을 채택하는 특성을 반영한다.

3.2 대역폭(Bandwidth) 허위 보고

토르 네트워크에서는 3-hop 어니언 라우팅으로 인한 오버헤드를 최소화하기 위해, 클라이언트가 높은 대역폭을 가진 릴레이를 선택하여 회로를 구성할 확률이 높도록 설계되어 있다. 따라서, 공격자는 본인이 소유한 악성 릴레이가 클라이언트로부터 입구 또는 출구 릴레이로 선택될 확률을 높이기 위해 릴레이의 대역폭을 매우 높게 보고할 수 있다. 이 경우, CPU/메모리 사용량이 보고된 대역폭에 비해 낮게 기록될 가능성이 있다. 또한, 등록한 릴레이 외 다른 릴레이의 설정 파일(torrc 파일)이 다수 존재할 경우, 악성 릴레이가 네트워크에서 차단될 시 다른 릴레이로 대체하기 위한 것으로 의심할 수 있다.

4. 결론

본 논문에서는 토르 네트워크에서 악성 릴레이를 탐지하기 위한 방법을 분석하고, 악성 행위에 따른 릴레이의 특징을 규명하였다. 특히, C&C(Command & Control) 서버와의 비정상적인 통신 패턴, 신뢰할 수 없는 SSL 인증서 사용, 짧은 연결 시간, 대역폭 허위 보고 등의 특징이 악성 릴레이를 식별하는 주요 지표가 될 수 있음을 확인하였다. 이러한 특징은 정상 릴레이와의 명확한 차이점을 제공하며, 이를 활용하여 토르 네트워크 내 악성 릴레이를 탐지하고 차단함으로써 익명성 기반의 보안을 강화할 수 있을 것으로 기대된다. 다만, 악성 릴레이의 행위가 점차 진화하고 있어 기존 탐지 방식만으로는 완벽한 방어가 어려운 한계가 존재하며, 실제 운영 환경에서의 적용 가능성과 효율성에 대한 추가적인 검증이 필요한 상황이다. 이 점을 고려하여, 향후에는 본 연구의 행위 특성 분석 결과를 바탕으로 실시간 대응이 가능한 탐지 체계를 설계하고 실제 환경에서의 적용 가능성을 함께 평가하는 방안을 모색하고자 한다.

참고문헌

[1] https://www.torproject.org/

[2] https://2019.www.torproject.org/about/overview.html.en#overview

[3] M. A. Irsyad Mohd Aminuddin, Z. F. Zaaba, A. Samsudin, N. B. Anuar Juma'at and S. Sukardi, "Analysis of the Paradigm on Tor Attack Studies", 2020 8th International Conference on Information Technology and Multimedia (ICIMU), Selangor, Malaysia, 2020, pp.126-131.

[4] https://www.malwarebytes.com/blog/news/2021/12/was-threat-actor-kax17-de-anonymizing-the-tor-network